2007-09-00

Use of EMS Personnel as Intelligence Sensors Critical Issues and Recommended Practices

Petrie, Michael

Monterey, California. Naval Postgraduate School

THE USE OF EMS PERSONNEL AS INTELLIGENCE SENSORS: CRITICAL ISSUES AND RECOMMENDED PRACTICES

Michael Petrie

INTRODUCTION

The use of Emergency Medical Services (EMS) personnel[1] as intelligence sensors or information collectors to provide information to Terrorism Early Warning Groups (TEWGs) and other local and state government intelligence fusion centers is recommended by numerous academic papers, professional articles and presentations, and U.S. Department of Homeland Security best-practice documents. These documents identify EMS personnel as valuable intelligence sensors, in part because they have access to locations not routinely available to law enforcement or intelligence communities that may contain indicators of terrorism.[2]

In spite of these recommendations, exceptionally few TEWGs have incorporated EMS personnel into their information collection systems. While many TEWGs are interested in integrating EMS collection assets, they have not developed this capability because they are confounded by the complex legal, operational, professional, cultural, and societal challenges of using EMS personnel in this capacity. Conversely, at least one intelligence fusion center developed an EMS-based information collection system, but overlooked federal and state medical confidentiality laws and other strategic issues.[3]

There has been no significant debate among federal, state, and local intelligence, EMS, law enforcement, homeland security, and medical communities regarding the best practices and strategic consequences of using EMS personnel as intelligence sensors.[4] Absent an such an interdisciplinary debate leading to the development of model EMS information collection practice standards and the articulation of clearly defined public benefit, elected officials, the leadership of the EMS and medical communities, and other policymakers will not sanction the use of EMS personnel in this capacity, resulting in the inability to use EMS personnel as information collectors to prevent terrorism.

Best practices for using EMS personnel as intelligence sensors must be developed because: (1) numerous TEWGs want to integrate EMS personnel as information collectors; (2) in the absence of peer-reviewed best practices, some TEWGs are instituting information collection practices that breach federal or state medical confidentiality laws, which may result in the unlawful disclosure, reception, and use of protected health information; (3) there are material civil, administrative, and criminal penalties for the improper disclosure, reception, or use of protected health information; and (4) ad hoc collection practices that breach the public's trust and expectation of medical confidentiality may result in the loss of this valuable collection asset or the creation of inordinately risk-averse TEWG oversight mechanisms.

In addition to discussing the strategic and legal issues and recommending practices for the use of EMS personnel as information collectors to support intelligence fusion centers, this article aims to stimulate debate among the intelligence, EMS, homeland security, law enforcement, and medical communities regarding the role of EMS personnel in supporting intelligence fusions centers.

THE VALUE OF EMS PERSONNEL AS INTELLIGENCE SENSORS

EMS personnel can function as high quality intelligence sensors. They respond to emergencies in residences and businesses owned, rented, or operated by all demographic groups in all geographic areas on short notice, usually arriving within eight minutes of the request for service. In many instances, the reporting party does not have time to "clean" the scene; thus indicators of terrorist ideology, planning, or operations may be visible when emergency responders arrive. Additionally, most people do not react defensively to EMS personnel and may not perceive a need to clean the scene. Patients seeking medical care may be unable to disguise suspicious injuries associated with the logistics of terrorism, such as burns or other trauma from chemical agents or explosives. EMS personnel carrying discreet chemical or radiological detection devices could provide the ability to check sites throughout a jurisdiction for potential precursors to terrorism that would otherwise be difficult to assess.

The use of EMS personnel as information collectors would markedly increase the number of intelligence sensors in the community and the number of contacts capable of yielding information. In one major west coast city, with a population of approximately 780,000, there are more than 2,000 fire department and ambulance personnel who respond to more than 80,000 EMS calls annually.[5] While the range of calls varies greatly by jurisdiction, a rough estimate is an annual average of 800 to 1,000 EMS calls per 10,000 population.

EMS personnel are well versed at determining the veracity of statements and patient histories, especially in situations when the stated history is inconsistent with the signs and symptoms or physical evidence. EMS personnel are skilled at recognizing dangerous or suspicious environments, and often have a good sense of community concerns due to their frequent interaction with the public.

Because EMS personnel often respond to calls in residences or businesses, they have access to the three traditional types of terrorism indicators: trait-based indicators, behavior-based indicators, and incident or site-based indicators. Trait indicators are based on an individual's or community's characteristics, such as race, religion, ethnicity, or national origin.[6] The use of these indicators has numerous limitations, including high rates of false positives and false negatives, engendering distrust between government and target communities, and a perception of racially, religiously, or ethnically-based persecution. Behavioral indicators are based upon persons' or communities' activities, conduct, or behaviors, rather than their characteristics.[7] Incident or site indicators are based upon what can be observed, heard, or otherwise sensed. Incident-based indicators are particularly valuable because they can identify evidence of terrorist ideology, planning, and operations. Ideological indicators include pictures, flags, or literature representing terrorists or terrorist organizations. Planning indicators include photographs or plans of critical infrastructure and detailed information about high-value sites. Operations indicators include weapons, explosives, chemicals, or timing devices. For EMS personnel, incident-based indicators do not include the patient's complaint, history, signs, or symptoms. These are considered medically-based indicators, which EMS personnel identify as part of their patient assessment.

Despite the potential benefit of using EMS personnel as intelligence sensors, a number of strategic questions must be considered. Will EMS personnel want to function as intelligence sensors? Will using EMS personnel as intelligence sensors conflict with society's expectations of medical professionals? Will using EMS personnel to collect

terrorism information reduce the total terrorism information received or reduce the number of calls for EMS service? Will using EMS personnel as information collectors violate medical confidentially laws?

EMS PERSONNEL ISSUES

Pre-hospital personnel will have varied reactions to serving as intelligence sensors to support intelligence fusion centers. Some EMS personnel will embrace this responsibility, believing it supports a safer community and nation. Others will avoid this responsibility because they believe it creates new risks and may interfere with their primary emergency medical care mission. These strategic issues deserve careful evaluation.

Serving as an information collector to support an intelligence fusion center is not without risk to individuals, their coworkers, organizations participating in the program, and the EMS discipline generally. Individual responders may place themselves and their coworkers at risk of physical harm, if terrorists or criminal organizations perceive that responders are providing information to law enforcement or intelligence fusion centers. EMS personnel commonly do not report contraband, illicit items, or violations of the law to law enforcement, unless there is an imminent threat to the rescuer; they do not want to be considered law enforcement informants, a perception that could leave them vulnerable to reprisals on future emergency responses.[8] Criminal informants, if identified, often need protection and their careers may end.[9] Emergency response personnel who are perceived as informants could be summoned to an ambush or other form of reprisal with a phone call.

Even if only a few EMS personnel participate in a collection program, a risk could be created for all personnel in that organization, as the public or targets will not necessarily differentiate between those who are participating and those who are not. However, the risk of reprisals against EMS personnel can be minimized if they collect and report only indicators of terrorism, not indicators of criminal activity. Even if terrorists suspect that EMS personnel are intelligence sensors, clandestine terrorist organizations planning or supporting an attack in America are unlikely to threaten or assail a paramedic, because to do so would attract the scrutiny of law enforcement. Many jurisdictions will determine that this possible risk to EMS personnel is outweighed by the opportunity to identify a terrorist's planning or operations by using EMS personnel as intelligence collectors. While that determination may be appropriate, the potential risk to EMS personnel must be carefully considered.

Intelligence gathering by pre-hospital personnel may interfere with traditional medical and health care missions. Two foundational principles of medical care are that clinicians will provide care without moral judgment and hold sacrosanct information provided by a patient. Medical confidentiality seeks to maximize patient communication with medical professionals, so that fear of disclosure will not deter people from seeking medical help and securing a diagnosis and adequate treatment. Medical confidentiality also seeks to encourage medical professionals to be candid in recording information in patient medical records, and to protect patients' privacy against disclosure of sensitive personal information.[10] Many clinicians believe that because of these principles, patients seek care they would otherwise decline if the circumstances of the care were disclosed. [11] Some EMS personnel consider that reporting patient information (provided to them with an expectation of privacy) to TEWGs violates these health care principles and

refuse to provide that information – even if that information prevents or preempts a potential terrorist attack. Disaffected EMS personnel may refuse to participate in a collection program, provide disinformation to fusion centers, or become "whistle blowers." (During the author's presentation on this subject, to approximately 100 pre-hospital personnel, most were interested in participating in an information collection program. However, about twenty-five attendees stated they would not, under any circumstances, participate in such a program.)[12]

SOCIETAL EXPECTATIONS OF EMS PERSONNEL

The American public expects privacy from their medical practitioners and feels strongly that health information and medical records are confidential and must not be released to others without the patient's permission.[13] Citing a Louis Harris poll, Beth Givens, director of the Privacy Rights Council noted that "In 1995, 82% of those polled, or four out of five, said they are somewhat or very concerned about threats to their personal privacy. This is up from 64% in 1978". Mainstream privacy groups identify secondary use of medical information without the patient's permission by unrelated third parties, including law enforcement, as "privacy abuse."[14] Absent compelling research to the contrary, we can presume that the public's expectation of privacy extends to EMS professionals. This expectation is certainly legitimate, as EMS personnel are included in the federal and exemplar state medical confidentiality laws.

If EMS participation in information collection and reporting programs is publicly known, members of the public, especially within marginalized communities, may believe they are being spied upon by pre-hospital personnel. This will breach the public's expectation of medical confidentiality and exacerbate distrust of the government, which may result in members of those communities refusing to use emergency services. Preventable morbidity and mortality would result if segments of the public stopped using emergency medical services or other health services. This is an utterly unacceptable consequence, which would require termination of the EMS collection and reporting program.

The use of EMS personnel as information collectors also involves issues similar to the community-based policing versus proactive or intelligence policing dichotomy. Advocates of community-based or crime-response and prevention policing believe intelligence gathering by police will interfere with their traditional crime-fighting and social-services mission.[15] This argument asserts, in part, that using police for intelligence purposes may alienate those communities that are the target of the intelligence operations, which may result in the alienated communities becoming less likely to report criminal activity or cooperate with police investigations, which correlates with higher rates of crime.[16] When applied to using EMS personnel as information collectors, this issue considers whether the government's use of individuals who are expected to maintain medical confidentiality as intelligence sensors is strategically counterproductive. The use of EMS personnel as intelligence sensors may be interpreted by certain communities as evidence that they are under constant surveillance and not trusted. This could engender community distrust, causing potential leads – that might otherwise be reported – to not be reported, resulting in a decrease of terrorist-related information from those communities.

Finally, another risk of using any non-law enforcement information sources, including EMS personnel, as information collectors is that alienated communities will

request redress from government policymakers. Municipal, county, or state policymakers may refuse to support the use of non-law enforcement personnel as information collectors, prohibiting those personnel from performing intelligence collection functions, or sanctioning those organizations through legislative or budgetary controls.

LEGAL ISSUES

Because TEWGs and other fusion centers have historically not used medical personnel as collection assets, the federal and state medical confidentiality laws and state mandatory reporting laws that relate to EMS personnel have not been relevant to their operations. However, it is critical that EMS personnel, EMS employers, and TEWGs that utilize EMS collection assets understand these laws, because they define the circumstances under which confidential medical information may be disclosed, received, or used.

Within the United States, a patient's[17] health information is protected from unauthorized disclosure, reception, or use through a rubric of federal and state laws. The Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule prescribes the federal requirements to protect the privacy of patients' health information and defines specific exemptions for disclosure of that information. In addition to the federal protections afforded by the HIPAA Privacy Rule, each state has a confidentially of medical information law that provides specific protections for medical and health information. Finally, each state has laws that compel health care providers and others to report to governmental agencies acts or conditions that identify abuse, crimes, or threats to public health and safety.

This article examines the HIPAA Privacy Rule and the confidentiality and mandatory reporting laws from the State of California for two reasons: California has a number of established intelligence fusion centers and the author is familiar with EMS operations in California. Not all the laws reviewed in the context of this article will apply to all states or agencies.[18]

The HIPAA Privacy Rule

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated the development of standards to protect the privacy of individually identifiable health information held or transmitted by a covered entity or its business associates in any form, including electronic, paper, or oral.[19] These standards are contained in the Standards for Privacy of Individually Identifiable Health Information, commonly called the HIPAA Privacy Rule or Privacy Rule.[20] The purpose of the Privacy Rule is to prevent the unauthorized disclosure of a patient's protected health information and define the specific circumstances when protected health information may be disclosed or used, with or without authorization. The Privacy Rule applies to "covered entities," which generally includes health plans and health care providers that transmit health information electronically for claims or billing, benefit eligibility inquiries, or referral authorization requests.[21] Nearly all public and private sector ambulance providers and first response agencies that bill government sponsored or other health plans for services are considered covered entities.

The Privacy Rule mandates that a covered entity must disclose protected health information in two situations: to patients or their representatives when they request

access to that information or to the U.S. Department of Health and Human Services when it is conducting an investigation or taking enforcement action. The Privacy Rule also permits, but does not compel, the covered entity to use or disclose protected health information without the patient's authorization in five categories of situations. One of these categories of situations – specific public interest and benefit activities – contains two lawful disclosure uses that authorize health care providers, including EMS personnel, to release protected health care information to law enforcement.[22] These lawful disclosure uses are (1) supporting specific law enforcement purposes and (2) to prevent or lesson the threat to serious health or safety.[23]

Covered health care providers providing emergency care at the scene of a medical emergency that is not on the provider's premises may disclose protected health information to law enforcement to alert law enforcement to the commission or nature of a crime, the location of a crime and its victims, or to report the identity, description, or location of the perpetrator of the crime.[24] This provision relates directly to EMS personnel; they are the only health care providers who routinely provide emergency medical care at locations other than their own premises.[25]

Covered health care entities, consistent with law and ethical conduct, may also use or disclose protected health information when the health care provider believes the use or disclosure "is necessary to lessen a serious and imminent threat to the health and safety of a person or the public" and the disclosure is made to a person able to prevent or lessen that threat.[26] This disclosure is presumed to be made in good faith if the health care provider relied on assertions made by a person who could credibly have knowledge of a threat to public health and safety.[27] This authorization supports EMS personnel informing law enforcement or TEWGs about potential terrorist threats, based upon a patient's history or statement, or signs and symptoms, provided the EMS personnel believe the patient's actions pose a serious and imminent threat to public health and safety and the law enforcement officer or TEWG is able to prevent or lessen the threat. In the situation of a terrorist being injured while manufacturing an improvised explosive device or chemical agent, reporting protected health information to law enforcement is justified – the person has already created a serious and imminent threat, has caused an injury to him/herself, has placed on-scene public safety personnel at risk, and may be creating a serious and imminent threat to the public.[28]

The Privacy Rule also allows the disclosure and use of protected health information for specialized governmental functions, including national security and intelligence activities. Pursuant to this exemption, a covered entity may disclose protected health information to authorized federal officials to support intelligence, counterintelligence, and other national security activities.[29] Disclosures made to authorized federal officials for national security or intelligence purposes are also exempted from a Privacy Rule requirement that covered entities identify all disclosures of protected health information made during the past six years, including disclosures to non-federal law enforcement agencies, upon the request of the patient.[30] These disclosure and reporting exemptions provide a method for FBI Joint Terrorism Task Forces, and similar organizations using federal officials, to confidentially access protected medical information that may contain indicators of terrorism, after receiving an initial lead from a TEWG or other source.[31]

HIPAA provides criminal and civil penalties for failure to comply with the Privacy Rule. The U.S. Department of Health and Human Services may fine covered entities up to one hundred dollars per occurrence for failing to comply with the Privacy Rule, and

up to a maximum of $25,000 annually for repeated violations of the same requirement. A person who knowingly discloses or uses individually identifiable health information may be criminally fined up to $50,000 and imprisoned for up to one year. If the illegal conduct involves false pretenses, the maximum fine increases to $100,000, and possible imprisonment increases up to five years. If a person unlawfully sells, transfers, or uses individually identifiable health information for commercial gain, the maximum fine is $250,000 and the maximum imprisonment is ten years. Criminal sanctions to enforce the Privacy Rule can only be applied by the U.S. Department of Justice.[32]

State Confidentiality of Medical Information Laws

In addition to understanding the requirements of the federal HIPAA Privacy Rule, EMS personnel, their employers, and TEWGs that use EMS personnel as intelligence sensors must understand the requirements of their state's medical confidentiality laws and mandatory reporting laws to comprehend what information may be legally reported to TEWGs. The content of these laws varies greatly by state, but generally identifies who is covered by the law; prohibits the release, sharing, or disclosure of medical information without the patient's permission; and identifies specific exemptions when information must or may be disclosed without the patient's authorization. [33]

In California, the primary medical privacy law is the California Confidentiality of Medical Information Act.[34] This law applies to all licensed or certified health care professionals, including physicians, nurses, emergency medical technicians (EMTs), and paramedics. The law also applies to organizations that store medical information, and organizations that employ health care personnel, such as EMS first responder agencies and ambulance providers.[35]

The California Confidentiality of Medical Information Act states, "No provider of health care, health care service plan or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care services plan without first obtaining an authorization."[36] The Act broadly construes medical information to include *any* element of information that allows identification of the individual, alone or when matched with other publicly available information.[37] Thus, except for defined exemptions, the Act comprehensively prohibits the release of a patient's medical information, including information which could be correlated with dispatch records or other public information to allow identification of the patient, without the patient's authorization.

The Act contains nine exemptions that compel covered entities to release information without a patient's authorization. These exemptions are limited to actions taken pursuant to court orders, subpoenas, investigations by agencies with regulatory oversight, search warrants, requests by a coroner under specific conditions, and when required by law.[38] The Act also contains eighteen exemptions when health care providers or others *may* disclose patient information. These conditions include furthering the treatment of patients among medical providers in emergencies, facilitating the payment of medical bills when the patient is unable to give authorization, allowing review and oversight by licensing and accrediting bodies, facilitating clinical research, supporting coroners' investigations, evaluating insurance plan coverage, determining the need for conservatorship, and supporting post-death organ transplant. Additionally, demographic information may be provided to a disaster relief organization to respond to welfare inquiries. Medical information may also be disclosed to a local

health department to assist in the prevention or control of diseases, and to support public health surveillance, investigations, and interventions.

None of these compulsory or permissive disclosure provisions allow EMS providers to release a patient's medical information to law enforcement or to a TEWG, even if that medical record suggests activities consistent with terrorist ideologies, planning, or operations. While EMS personnel could disclose medical information to EMS regulatory agencies, such as local EMS agencies,[39] these agencies are prohibited from disclosing that information to parties that are not otherwise authorized to receive or use that information.[40]

The California Confidentiality of Medical Information Act provides criminal and civil penalties, including compensatory and punitive damages, for unauthorized disclosure of medical information in violation of the Act.[41] (Other state laws provide additional remedies.) The civil, administrative, and criminal penalties for violating the California Confidentiality of Medical Information Act are severe. In the context of EMS personnel releasing medical information to law enforcement or TEWGs in violation of the Act, the penalties could be applied against the person unlawfully disclosing the information, against the employing agency, and against the TEWG for unlawfully receiving or using the information. For EMS personnel, a criminal conviction under this act will probably cause the revocation of their license, termination of their employment, and end their careers.[42] For the TEWG organization, a criminal conviction under this act would result in scrutiny that would threaten the viability of the organization and the local and state intelligence fusion center concept.

State Mandatory Reporting Laws

Like other states, California has laws that require health care providers to report certain acts of violence to local law enforcement and certain diseases to the public health officer. While pre-hospital personnel are not required to report under either of these laws, they are relevant because many EMS personnel erroneously believe these laws allow them to report otherwise confidential information to law enforcement.

California Penal Code Section 11160 provides that health practitioners employed in certain facilities, or employed by a local or state public health department, must report to a law enforcement agency any patient who presents with injuries that are self inflicted, inflicted by another with a firearm, or that appear to be the result of actual or attempted assault or abusive conduct. (Assault or abusive conduct includes any of twenty-three crimes, including manslaughter, torture, battery, incest, rape, throwing any caustic chemical with intent to injure, child abuse or endangerment, abuse of spouse, lewd acts with a child, and elder abuse.) The content of the report made by the health practitioner to law enforcement is not limited, and could reasonably include the patient's medical record, which would otherwise be confidential.[43] This law applies only to the specific health care providers identified within the law, which does not include EMTs and paramedics (EMS personnel). Thus, EMS personnel in California may not release confidential medical information directly to law enforcement or a TEWG. However, hospital-based physicians and nurses are compulsory reporters under this law. Information reported by EMS personnel to hospital personnel is reportable by hospital personnel to law enforcement as part of this law's compulsory reporting requirements, making the interpretation of this law relevant to how EMS personnel could report medical information that may indicate terrorist planning and operations.

California Code of Regulations, Title 17, Section 2500 requires certain health care providers, including physicians, mid-level practitioners, nurses, infection control personnel, but not EMS personnel, to report to the local health officer in which the patient resides, any of eighty-eight diseases or conditions. These diseases include the Category A Bioterrorism Agents and diseases on the Centers for Disease Control and Prevention's list of Bioterrorism Agents and Diseases.[44] When no health care providers are present, any person aware of an individual suspected to be suffering from any of the covered diseases may notify the health officer.[45] While EMS personnel are not mandatory reporters, they may permissively report a patient suspected of these diseases to local health authorities in the absence of a compulsory reporter. This law does not allow EMS personnel to report this information to TEWGs or law enforcement.

Other California laws and regulations compel reporting of confidential medical information to law enforcement, public health, and environmental health authorities. Emergency medical technicians and paramedics must report child abuse and dependent elder abuse.[46] However, within the performance of their pre-hospital duties, this reporting, while essential to protect public safety, does not provide a mechanism to report medical information or signs and symptoms that could indicate planning or other preparation for terrorism.

Evaluating the Legal Rubric

To determine how medical confidentiality and disclosure laws affect the ability of EMS personnel to provide information to intelligence fusion centers, the HIPAA Privacy Rule and state confidentiality and disclosure laws must be jointly analyzed. Except for specific exemptions, the HIPAA Privacy Rule preempts contrary portions of state law.[47] The Privacy Rule provides two principle exceptions to the general rule of federal preemption. These exceptions apply if the state law: (1) more stringently protects health information or grants the patient greater access to his or her health information; or (2) provides for the reporting of certain diseases or injury, child abuse, or public health surveillance, investigation or intervention.[48] This preemption test creates a floor or minimum standard for protection of medical information. If a state law provides a higher level of medical privacy, the level created by the state law applies. State laws for reporting disease, criminally-caused injury, or public health investigations are not preempted. [49] There are other exceptions to preemption, which are not relevant to this discussion.

Section 164.512(f) (6) of the HIPAA Privacy Rule allows EMS providers, in response to a medical emergency that is not on the EMS provider's premises, to disclose protected health information to law enforcement, if that disclosure is necessary to alert law enforcement about the commission and nature of a crime, the location of the crime or its victims, or the identity of the perpetrator of the crime.[50] Section 164.512 (j) of the Privacy Rule allows EMS providers to use or disclose protected health information when the health care provider believes the disclosure is necessary to lessen a serious and imminent threat to the health and safety of a person or the public and the disclosure is made to a person able to prevent or lessen that threat.[51] Section 164.512(k)(2) of the Privacy Rule permits EMS personnel to disclose protected health information to authorized federal officials to support intelligence, counter intelligence, and other national security activities.[52]

None of these provisions preempt the California Confidentiality of Medical Information Act's prohibition against unauthorized use or disclosure of a patient's health information because the state law more stringently protects that information. Thus, EMS personnel in California may not report confidential medical information to law enforcement or a TEWG to alert law enforcement about the commission and nature of a crime, the location of the crime or its victims, or the identity of the perpetrator of the crime, or to lessen a serious and imminent threat to the health and safety of a person or the public. Nor may EMS personnel report confidential medical information to authorized federal officials to support intelligence, counter intelligence, and other national security activities.[53]

California law is generally more severe than the Privacy Rule regarding sanctions for unlawfully disclosing health information, and is not preempted by HIPAA. For some specific violations, such as unlawful disclosure of protected health information under false pretenses, the Privacy Rule's penalties are harsher. In these situations, the harsher penalty would be applied. For a case to be made under the Privacy Rule there must be specific intent to violate the law. For a case to be made under California law, only negligent disclosure is necessary. Under the Privacy Rule, an action must be brought by the U.S. Department of Health and Human Services or the U.S. Department of Justice; however, under the California Confidentiality of Medical Information act, an individual patient or numerous governmental attorneys may initiate legal action.[54]

In summary, the exercise of the three lawful disclosure provisions in the HIPAA Privacy Rule that allow EMS personnel to disclose protected health information to law enforcement are prohibited by the more stringent requirements of the California Confidentiality of Medical Information Act. Furthermore, in California there are no mandatory reporting laws that allow EMTs and paramedics (EMS personnel) to report medical indicators of terrorism to law enforcement or a TEWG. Disclosure of protected medical information carries heavy penalties; the HIPAA Privacy Rule and the California Confidentiality of Medical Information Act provide material sanctions for those who use or disclose protected health information without authorization.

Therefore, EMS personnel are not allowed to report confidential medical information to law enforcement or a TEWG, even if that information suggests terrorist planning or operations. The inability to report confidential medical information creates ethical and moral challenges for the paramedic who discovers medically-based indicators of terrorism that she believes should be reported to law enforcement. These professional, societal, and operational issues are examined in the balance of this article.

RECOMMENDATIONS

Although the use of EMS personnel as information collectors may be controversial, there is a realistic probability that an EMS responder at the scene of a medical emergency may provide information to prevent, preempt, or interdict a terrorist attack. Based on the evaluation of each issue identified in this article, the use of EMS personnel in this capacity is both ethical and legitimate, given certain constraints.

EMS personnel should only collect and report incident-based indicators and non-medical behavior-based indicators of terrorism to TEWGs. This information, which does not include protected health information, is high-value information. Incident-based indicators have low rates of false-positive and false-negative leads, because collectors can clearly articulate what they observe and why it is suspicious. In response to a call for

medical assistance, a paramedic enters a residence and observes a case of Casio watches, soldering irons, wiring, and numerous suitcases. A paramedic who has received terrorism awareness training would understand that the wiring and the number of watches are suspicious and potentially related to terrorism because they can be used to construct time- or altitude-triggered detonators. Furthermore, when considered with the watches and wiring, the suitcases are suspicious because they could be used to covertly deploy explosive devices on planes or aircraft.

Behavior-based indicators of terrorism may also be valuable, but are often less specific than incident-based indicators of terrorism. A paramedic responds to a residence for a middle age male complaining of severe chest pain and shortness of breath—a potential heart attack. The paramedic notes that two men try to delay his access to the patient, while two other men speak quickly in hushed voices to the patient, and then rapidly and anxiously leave the residence. A paramedic who has received terrorism awareness training might report this behavior to the local TEWG, especially if incident-based indicators of terrorism were also present. However, it would be difficult to determine whether this behavior, which could be considered suspicious, has any link to terrorism.

Incident-based and non-medical behavior-based information can be fused with publicly available information, such as dispatch records, to create valuable intelligence. This practice will result in EMS personnel providing a manageable quantity of high-quality information inputs into the intelligence collection, fusion, and analysis process.

The release of confidential medical information by EMS personnel to TEWGs adds little value to the intelligence fusion process. A suspicious injury (such as burns to both arms) and an implausible history not consistent with the injury only indicate the patient burned his arms other than described, not that the burns were specifically related to terrorist activities. While medically-based indicators such as injuries with inconsistent histories *may* indicate terrorist-related activities, it routinely indicates a patient's attempt to cloak the ridiculus and embarrassing – yet lawful – circumstances of an injury. Reporting every inconsistent physical presentation and history that might suggest terrorism would generate many false-positive leads, which would exhaust analysts' time and cloud the database with misleading data, reducing the acuity of the analysis. Similarly, depending on pre-hospital personnel to report clinically-based information from the pre-hospital setting would generate false-negative or missed leads, because EMS personnel cannot reliably differentiate diseases associated with bioterrorism from other routine diseases or ascribe the etiology of many injuries.

Even when supported by state and federal law, EMS personnel should not disclose protected health and medical information to law enforcement or TEWGs, at least until such time as there has been a dialogue on the role of EMS personnel serving as information collectors. The release of a patient's protected medical information is contrary to the societal expectations of privacy and the medical profession's fundamental ethical principle of patient privacy.[55] Absent a national interdisciplinary dialogue, medical professionals and the public will consider the release of patients' confidential medical information, by EMS personnel to TEWGs, a serious ethical breach.

Further, reporting clinical information from the pre-hospital setting is not necessary, because it is available elsewhere. State mandatory reporting laws require hospital-based

personnel to report many clinical indicators of terrorism, including injuries that suggest violence against a person, to law enforcement.

Recommendation 1: Develop Stakeholder Support and Identify Standards and Best Practices

If programs using EMS personnel as intelligence sensors to support intelligence fusions centers are implemented nationally, the U.S. Department of Homeland Security and the U.S. Department of Health and Human services should convene medical intelligence working groups to develop collection standards and to clarify regulation. These groups should advocate the collection and sharing of information that could identify terrorist planning or operations, while protecting the health and medical privacy rights of all patients. Working groups need to include representative organizations from the state and local intelligence, law enforcement, EMS, legal, and medical communities, specifically including medical ethicists. While this type of collaborative process may appear unnecessary or counterproductive to representatives from established intelligence fusion centers, EMS or medically-based information collection programs developed surreptitiously or without the support of stakeholder communities are likely to fail amid political scandal. Print and electronic media records are replete with reports of local and state governments involved in non-criminal intelligence or surveillance operations.[56] Common themes of these reports are allegations of "spying on the public," improper use of personnel, public demands for an investigation, replacement of high-level staff, and increased oversight. It is unlikely that the EMS profession or other medical professions, which are expected to protect patient confidentiality, would expose themselves to those potential charges, absent a national consensus.

Recommendation 2: Parameters for Program Development

Terrorism Early Warning Groups or EMS organizations wishing to develop an EMS-based information collection program to support intelligence fusion and analysis should approach this issue methodically. The following steps are recommended:

1. *Consult with the agency's legal counsel to review the HIPAA Privacy Rule, state confidentiality of medical information laws, state mandatory reporting laws, and related local laws or ordinances.* Determine how these laws will affect the EMS provider's information collection and reporting efforts.
2. *Identify and train at least one EMS agency Terrorism Liaison Officer (TLO).* The EMS agency's TLO will be the primary point of contact between the EMS organization and the TEWG. This person will assume responsibility for program development and operations, including initial and recurring staff training, vetting and reporting information to the TEWG, serving as the key point of contact for the EMS organization, and receiving intelligence products generated by the TEWG that the EMS agency has a right and need to know.
3. *Based on the advice of legal counsel, develop a proposed collection and reporting protocol.* This protocol should be cooperatively developed by the EMS organization and the TEWG. The protocol should be reviewed by the EMS regulatory authority to assure its use is authorized and employees' licenses or certifications will not be jeopardized by participation in the program. Employee labor organizations should review and comment on the protocol to address

labor's concerns and to garner support for the program. In organizations without organized labor representation, employee review can be accomplished through vertically- and horizontally-structured employee groups that include formal and informal organizational leaders.

4. *Secure the support of appropriate policy makers*. Based on local norms and the direction of executive personnel, the program may be reviewed by elected officials or community leaders. Organizational leaders must determine whether the public disclosure or dialogue about the use of EMS personnel as intelligence sensors increases the probably of the program's long term success.
5. *Develop the EMS organization's information collection program*. The EMS collection program must include structures and processes for the effective and timely transfer of EMS field personnel's observations to the TEWG. In addition to training staff, this will include developing policies to report information, standardizing paper reporting forms or database reporting templates, and reviewing processes. These systems should be developed leveraging the expertise of the EMS organization, the TLO, and the TEWG. While outside the scope of this article, well-designed reporting forms can fully mitigate the inability to access medically-based indicators of terrorism that EMS personnel may not lawfully disclose to TEWGs.
6. *Allow employees to confidentially opt into the information collection program*. Requiring employees to opt into the program reinforces that participation is voluntary. While employees may identify participants and non-participants through attendance at trainings or while reporting, the goal is to allow employees to participate or not participate without experiencing overt or indirect pressure from peers or management, which may result in attempts to sabotage the program.
7. *Train participating EMS personnel as information collectors*. Field-level EMS personnel should be trained to collect information, through an EMS-specific program. The training curriculum must provide learners with competencies to: (a) understand the role and responsibilities of EMS personnel in information collection to support intelligence fusion and analysis; (b) identify the benefits, limitations and issues of different types of indictors of terrorism, such as trait-based indicators, behavior-based indicators, site- or incident-based indicators, and medical-based indicators; (c) recognize incident- or site-based indicators of terrorism planning and operations; (d) articulate the legal and ethical issues associated with medical confidentiality and protected health information; (e) understand the history, cultures, and beliefs of various terrorist organizations; and f) be aware of local terrorism issues.
8. *Develop a comprehensive public information plan that explains why EMS personnel are being used in this capacity*. This should be a joint effort, between the TEWG or fusion center and the EMS agency. While a public information plan may seem counterproductive to a fusion center's goals, information about the collection program will become public. Charges of domestic spying and the associated negative public relations can be minimized if the collection program's

goals, legitimate rationale, and respect for privacy and medical confidentiality laws are disclosed in advance of the program.

Recommendation 3: Summary EMS Information Collection Protocol

Before beginning an EMS information collection program, every organization should develop a protocol to prescribe practices for information collection and the organization's review and referral of that information. While presenting an EMS organization's comprehensive information collecting and reporting protocol is beyond the scope of this article (it must incorporate a specific organization's legal analysis and operational structures and processes), such a protocol should minimally consider the following elements:

Awareness

- EMS personnel should be alert to incident-based indicators of terrorism on *every* call, including vehicle accidents and calls to residences, businesses, and public spaces.
- EMS personnel should be alert to the behavior of those on scene, including family and friends of the patient.

Information Collection

- EMS personnel should only collect and report scene- or incident-based indicators of terrorism.
- EMS personnel should continue to report or not report indicators of non-terrorism related crime, as determined by agency or personal practice.
- Confidential medical information should not be released or disclosed to law enforcement or TEWGs, unless compelled by mandatory reporting laws or legal order. (Confidential medical information includes the patient's signs, symptoms, current and past medical history, and communication with the patient, whether in written, oral, or other form.)

Reporting

- If indicators of terrorism are observed and responder safety is at risk, EMS personnel should call local law enforcement immediately or as soon as is safe.
- If indicators of terrorism indicate an attack is imminent, EMS personnel should call local law enforcement or the local 24/7 FBI Joint Terrorism Task Force (JTTF) immediately or as soon as is safe.
- Other indicators of terrorism should be routed through the EMS organization's TLO to the TEWG, as per protocol, using the organization's information reporting forms.

Confidentiality Verification and Process and Quality Improvement

At least quarterly, the TLO should examine the terrorism information reporting inputs, processes, and outputs to determine whether:

- There was any breach in patient privacy;
- Information was reviewed in a timely manner by the TLO and provided to the TEWG;
- Areas for improvement or successes were identified by information collectors;
- Any changes in the program are required.

Recommendation 4: Reform State Laws to Provide Consistent Mandatory Reporting Requirements for Medical Professionals

States should review their laws and mandated reporting requirements to assure consistency and, if possible, compatibility with HIPAA. For example, California's fragmented and incongruent compulsory reporting laws have disparate definitions of health care providers, resulting in a confusing arrangement of compulsory reporters for various injuries, diseases, and conditions. The variances in mandatory reporters contained within these laws are not rational. A paramedic employed by a local department of health has different reporting requirements than a paramedic employed by a fire department or private ambulance company.[57] A common definition of healthcare provider across these statutes and regulations would result in more uniform reporting and improved safety for the victims of crime and abuse.

CONCLUSION

EMS personnel can be valuable information collectors to support terrorism intelligence fusions centers. They can provide important information inputs that would not otherwise be available to fusion centers. However, every intelligence fusion center and EMS organization considering such a program must carefully analyze the legal, ethical, societal, and organizational issues unique to that EMS organization. Each EMS organization must use a methodical information collection implementation process, which includes legal analysis, developing a collection protocol, designating a terrorism liaison officer, designing a collection program, garnering employee support, training field employees, and assuring patient privacy.

In the longer term, the success and acceptance of the use of EMS personnel as information collectors to support terrorism intelligence fusion centers depends on significant dialogue among civilian intelligence, EMS, law enforcement, homeland security, and medical communities regarding the considerations, practices, and strategic consequences of using EMS personnel as intelligence sensors. Without this dialogue, the use of EMS personnel as intelligence sensors will not be sanctioned by the medical community or the public, most EMS systems and personnel will decline to serve as intelligence sensors, and important collection assets will be lost. The failure to deploy EMS personnel as information collection assets would be unfortunate, because there is a very real possibility that EMS personnel could provide critical clues to prevent, preempt, or interdict a terrorist attack in the United States, as they did to prevent the car bombing attacks in London on June 29, 2007.

As the administrator of the City and County of San Francisco Emergency Medical Services Agency, Michael Petrie is responsible for EMS System development, planning, regulation, and homeland security and disaster preparedness. He also serves on the faculty of the Center for Homeland Defense and Security at the Naval Postgraduate School. Mr. Petrie holds an MBA from the University of Phoenix and a master's degree in Homeland Security and Defense from the Naval Postgraduate School.

---

[1] For the purposes of this article, EMS personnel and pre-hospital personnel are used interchangeably. These terms denote non-law enforcement emergency medical technicians and paramedics who provide pre-hospital care from emergency response apparatus such as fire engines, ambulances or supervisory

vehicles. Law enforcement agency-based pre-hospital personnel are not included in this definition because, while they constitute a small, albeit important, portion of EMS personnel nationally, their law enforcement status presents unique issues regarding laws, enforcement responsibilities, and professional and societal expectations.

[2] Jim F. Morrissey, "Strategies for the Integration of Medical and Health Representation within Law Enforcement Intelligence Fusion Centers" (MA Thesis, Naval Postgraduate School, 2007), 45. U.S. Department of Homeland Security, Lessons Learned Information Sharing, *Local Anti-Terrorism Information and Intelligence Sharing: Information Analysis and Synthesis* (Washington, D.C., May 25, 2005), 1, www.llis.gov. Michael Grossman, *Terrorism Liaison Officer: Enhanced Intelligence Sharing, a Regional Solution* (October 2003), 3-5, www.llis.gov.

[3] The credible source for this and the prior sentence requested confidentiality.

[4] Thorough searches of academic and professional journals, homeland security portals and databases, and the National Library of Medicine's PubMed database failed to identify articles, instructions, recommendations, or best practices for EMS personnel providing information inputs to TEWGs.

[5] Glenn Ortiz-Schuldt, EMS Chief, San Francisco Fire Department, interview by author, San Francisco, August 9, 2004.

[6] Heather H. Davis and Gerard R. Murphy, *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement. Vol. 2: Working with Diverse Communities* (Washington, D.C.: Police Executive Research Forum, 2004), 10.

[7] Jonathan R. White, *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security* (Belmont: Wadsworth Townsend, 2004), 73.

[8] Chuck Whitmarsh, Firefighter/Duty Officer, East Bay Terrorism Early Warning Group, telephone interview by author, April 19, 2007.

[9] Stewart Field and Caroline Pelser, *Invading the Private: State Accountability and New Investigative Methods in Europe* (Aldershot: Ashgate Publishing, 1998), 40.

[10] New York City Health and Hospitals Corporation, Respondent, v. Robert M. Morgenthau, &c., Appellant (2002 NY Int. 113. 15), http://www.law.cornell.edu/nyctap/I02_0113.htm.

[11] John Brown, M.D., EMS Medical Director, City and County of San Francisco Department of Public Health, interview by author, San Francisco, August 16, 2004.

[12] Michael Petrie, "EMS Personnel as Intelligence Sensors," presentation to San Francisco Paramedic Association quarterly meeting, San Francisco, California, November 2006.

[13] Robert Gellman, "Health Privacy: The Way We Live Now," (Privacy Rights Council, August 22, 2002), http://www.privacyrights.org/ar/gellman-med.htm.

[14] Beth Givens, "Medical Records Privacy: Fears and Expectations of Patients" (Privacy Rights Council, May 19, 1996), www.privacyrights.org.

[15] White, *Defending the Homeland*, 6.

[16] Ibid., 24.

[17] As used in this paper when related to authorizing the release, use or disclosure of confidential medical information, the term "patient" includes the patient and his/her authorized representative.

[18] Agencies should consult their attorney before using EMS personnel to support an intelligence fusion center. Legal review is necessary to understand the effects of case law or interpretations on federal and state medical confidentiality laws, to identify local laws regulating the disclosure of protected health information, and to craft agency or departmental policies and procedures relating to the disclosure of protected health information.

[19] U.S. Department of Health and Human Services, Office for Civil Rights, *Summary of the HIPAA Privacy Rule* (Washington, D.C., May 2003), 3. U.S. Department of Health and Human Services, Office

for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information* (Washington, D.C., January 14, 2002), 6-10, http://www.hhs.gov/ocr/hipaa/finalmaster.html.

[20] Code of Federal Regulations, Title 45, Section 160,

[21] U.S. Department of Health and Human Services, *Summary of the HIPAA Privacy Rule*, 2.

[22] Ibid., 4.

[23] Code of Federal Regulations, Title 45, Section 164.512.

[24] Code of Federal Regulations, Title 45, Section 164.512(f)(6)(i).

[25] A licensed attorney reviewed this argument and requested confidentiality as the review was not in the course of his/her employment.

[26] Code of Federal Regulations, Title 45, Section 164.512(j)(1)(i).

[27] Code of Federal Regulations, Title 45, Section 164.512(j)(4).

[28] A licensed attorney reviewed this argument and requested confidentiality as the review was not in the course of his/her employment.

[29] Code of Federal Regulations, Title 45 Section 164.512 (k)(2)

[30] Code of Federal Regulations, Title 45, Section 164.528 (a)

[31] A licensed attorney reviewed this argument and requested confidentiality as the review was not in the course of his/her employment.

[32] U.S. Department of Health and Human Services, *Summary of the HIPAA Privacy Rule*, 17-18.

[33] David Humiston and Stephen M. Crane, "Will Your State's Privacy Law Be Superseded by HIPAA?" *Managed Care Magazine,* May 2002, 1, http://www.managedcaremag.com/archives/0205/0205.hipaabystate.

[34] California Civil Code Section 56-56.37.

[35] California Civil Code, Section 56-56.07.

[36] California Civil Code, Section 56.10 (a).

[37] California Civil Code, Section 56.05 (g).

[38] California Civil Code, Section 5610 (b).

[39] Local EMS Agencies as defined in California Health and Safety Code, Section 1797.24.

[40] California Civil Code, Section 56.10 (c) 5.

[41] California Civil Code, Section 56.35-56.37. Any patient whose medical information has been disclosed in violation of the Act may individually initiate litigation. Further, the State Attorney General and numerous local government attorneys may initiate civil action to assess a civil penalty. In addition to compensatory and punitive damages, there are administrative fines and civil penalties up to $2,500 per violation for negligently releasing confidential medical information, and administrative fines and civil penalties up to $25,000 per violation for willfully releasing confidential medical information. Persons and entities that unlawfully and willingly release, obtain or use confidential medical information for financial gain may receive administrative fines and civil penalties up to $250,000 per violation. Unauthorized persons or entities that willfully disclose, obtain or use medical information without authorization from the patient are liable for a civil penalty up to $250,000 per violation.[41] Any violation of the Act that results in economic loss or personal injury of a patient is a misdemeanor.
Humiston and Crane, "Will Your State's Privacy Law Be Superseded by HIPAA?"

[42] California Health and Safety Code, Section 1798.200.

[43] California Penal Code, Section 11160.

[44] U.S. Department of Health and Human Services, Center for Disease Control and Prevention, *Bioterrorism Agents/Diseases*, www.bt.cdc.gov/agent/agentlist-catefory.asp.

[45] California Code of Regulations, Title 17, Section 2500.

[46] California Penal Code, Section 11164-11174.3. California Welfare and Institutions Code, Section 15630-15632.

[47] Code of Federal Regulations, Title 45, Section 160.202-160.205. Humiston and Crane, "Will Your State's Privacy Law Be Superseded by HIPAA?"

[48] Code of Federal Regulations, Title 45, Section 160.202-160.203

[49] Georgetown University, Institute for Health Care Research and Policy, Health Privacy Project, *Summary of HIPAA Privacy Rule* (Washington, D.C., September 13, 2002), 34, http://www.healthprivacy.org/usr_doc/RegSummary2002.pdf.

[50] Code of Federal Regulations, Title 45, Section 164.512(f)(6)

[51] Code of Federal Regulations, Title 45, Section 164.512(j)(1)(i).

[52] Code of Federal Regulations, Title 45, Section 164.512 (k)(2)

[53] A licensed attorney and a HIPAA compliance officer reviewed this argument. Both requested confidentiality as the review was not in the course of their employment.

[54] Humiston and Crane, "Will Your State's Privacy Law Be Superseded by HIPAA?"

[55] D.Y Dodek and A. Dodek, "From Hippocrates to facsimile: Protecting patient confidentiality is more difficult and important than ever before," *Canadian Medical Journal* 156, no. 6 (March 15, 1997): 847-852.

[56] Nanette Miranda, "Did the National Guard Spy on 'Raging Grannies?'" *KGO ABC 7 News,* February 28 2006, 1, http://abclocal.go.com/kgo/story?section=politics&id=3949805. Staff, "Police Spies Chosen to Lead War Protest," *San Francisco Chronicle*. July 28, 2006.

[57] California Penal Code, Section 11160.